

Publication number: JP62015657 (A)

Publication date: 1987-01-24

Inventor(s): SUZUKI HIDEO

Applicant(s): CASIO COMPUTER CO LTD

Classification:

- international: G07F7/12; B42D15/10; G06K17/00; G06K19/077; G06Q20/00; G06Q40/00; G07D9/00; G07F7/10; H04M1/675; G07F7/12; B42D15/10; G06K17/00; G06K19/077; G06Q20/00; G06Q40/00; G07D9/00; G07F7/10; H04M1/66; (IPC1-7): G06F15/30; G06K17/00; G07F7/08

- European: G06K19/077; G07F7/10D6P; G07F7/10D8; H04M1/675

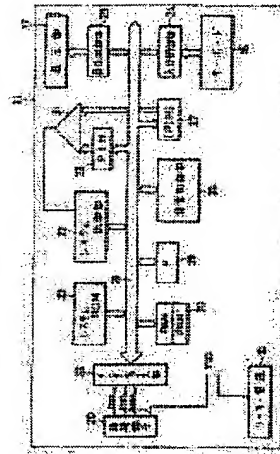
Application number: JP19850153637 19850712

Priority number(s): JP19850153637 19850712

Abstract of **JP 62015657 (A)**

PURPOSE: To approve the propriety of the owner of an IC card by providing a means inputting the character number information into the IC card in a no-connection state with an external device and collating the input information with the identification information on an identification memory within the IC card.

CONSTITUTION: When the IC card 11 is put into a card slit at an IC card terminal, the account number PAN and a ciphered account number PAN' sent from the card side are decoded at the terminal side. When the coincidence is obtained between the PAN and the PAN', it is decided that the card 11 is right. Then the card 11 is pulled out of the terminal and an identification number PIN is supplied by means of a PIN key through the keyboard 16 of the card 11.; Then the input PIN of a PIN latch part 28 is collated with the number PIN of the genuine card owner stored in a PIN memory 27 through an identification information comparing part 31. When the coincidence is obtained from this collation, it is decided that the input operator of the PIN key is identical with the genuine owner of the card 11.



Also published as:

JP8003821 (B)

JP2090978 (C)

US4742351 (A)

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭62-15657

⑪ Int.Cl.⁴

識別記号

庁内整理番号

⑬ 公開 昭和62年(1987)1月24日

G 06 F 15/30

8219-5B

G 06 K 17/00

6711-5B

G 07 F 7/08

B-7234-3E

審査請求 未請求 発明の数 1 (全9頁)

⑭ 発明の名称 ICカードにおける本人照合方式

⑮ 特 願 昭60-153637

⑯ 出 願 昭60(1985)7月12日

⑰ 発 明 者 鈴木 秀 夫 東京都西多摩郡羽村町栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内

⑱ 出 願 人 カシオ計算機株式会社 東京都新宿区西新宿2丁目6番1号

明 細 書

1. 発明の名称

ICカードにおける本人照合方式

2. 特許請求の範囲

外部装置との接続によりカード自体の正当性が調べられるICカードにおける本人照合方式において、上記ICカード内に設けられ所定文字数の暗証情報を予め記憶する暗証情報メモリと、上記外部装置との非接続状態においてのみ上記ICカードにて上記所定文字数の情報を入力可能とする手段と、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをICカード内にて比較照合する手段と、この比較照合手段による暗証情報の照合結果を出力する手段とを具備し、上記ICカードの正当性を確認すると共に、上記暗証情報が上記外部装置に一切入力されることなく、カード所有者の本人照合を行なうことを特徴とするICカードにおける本人照合方式。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、ICカードの正当性およびそのカード所有者が本人か否かを確実に照証するICカードにおける本人照合方式に関する。

〔従来技術とその問題点〕

近年はキャッシュレス時代と呼ばれており、クレジットカード会社等により発行されたカードを使用することにより、現金の取扱いをせずに商品の購入が可能となっている。上記カードとしては、従来、プラスチックカード、エンボスカード、磁気ストライプカード等が一般に使用されているが、これらのカードは構造上偽造が簡単であり、不正使用が問題になっている。このような問題を解決するため、最近ではカード内に、暗証番号等を記憶したIC回路を組み込み、暗証番号が外部から容易に読出せないようにした情報カード、所謂ICカードが開発されている。このICカードは偽造が困難で機密性に優れ、また、多数の情報を記憶できるという利点がある。しかして、上記のようなICカードを使用して実際取引を行なう場合

には、銀行あるいは商店等に設置したICカードターミナルにICカードを装着し、暗証番号等を入力してカードおよびカード所有者の正当性を確認した後、所定の処理動作が行なわれるようにしている。

しかしながら、このようにICカードをターミナルに装着して暗証番号の照合を行なう場合、第1に、例えば商店等において暗証番号を入力する際に、その入力操作自体を視覚によって盗まれる可能性がある。また、第2に、例えばターミナル側に、カード所有者によって入力される暗証番号の情報を、暗証番号一致の信号を持って記憶する細工が施してある場合、真のカード所有者の暗証番号が上記ターミナルの設置される商店主等によって、簡単に盗まれてしまう恐れもある。ここで、上記第1の問題点については、カード所有者自体がキー操作時に自分の暗証情報を盗まれないように気を付ければよいわけであるが、第2の問題点については、カード所有者側における対策は全く立てられないものである。

てしまうことなく、カード所有者の正当性を確実に認証することができるようになるICカードにおける本人照合方式を提供することを目的とする。
〔発明の要点〕

すなわちこの発明に係わるICカードにおける本人照合方式は、外部装置との接続によりカード自体の正当性が確認できるICカード内に、所定文字数の暗証情報を予め記憶する暗証情報メモリを設けると共に、上記外部装置との非接続状態において上記所定文字数情報の入力可能な手段を備えさせ、そして、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをこのICカード内にて比較照合し、その照合結果を出力するように構成したものである。

〔発明の実施例〕

以下図面によりこの発明の一実施例を説明する。

第1図はそのICカードにおける本人照合方式を実現したICカード11およびその外部装置(ICカードターミナル)12の外観構成を示す

そこで現在、カード所有者の暗証番号をカード発行時において予めカード内メモリに記憶させ、カード本体に設けたキーボードより入力される暗証番号と、上記メモリ内暗証番号とを比較照合し、その照合結果を即座にICカード自体に設けた表示部にて表示するようにした、所謂、ターミナル側とは全く接続関係を持たないで、独自に本人照合を行なうことのできるICカードが考えられている。しかし、このような単独にて本人照合を行なえる機能を有するICカードにあっても、そのカード自体が偽造される可能性がある。すなわち、カード本体上の表示部にて、例えば「本人OK」等の表示が行なわれたとしても、そのカード自体、真に正当のカード会社より発行されたものかどうかを確認することができないため、結局、真のカード所有者の認証を行なうのは非常に困難なものとなる。

〔発明の目的〕

この発明は上記のような問題点に鑑みなされたもので、カード所有者の暗証情報が不正に盗まれ

もので、本方式におけるターミナル12には、その本体上面にキーボード13、表示部14および上記ICカード11との電気的接続を図るためのカード挿入口15が設けられている。

第2図は、上記ICカード11の外観構成を示すもので、このICカード11には、その本体上面にキーボード16、表示部17およびソーラ電池18が設けられている。上記キーボード16は、テンキー、ファンクションキー等の演算用キーと共に、PINキー19を備えている。上記PINキー19は、本カード11とカード所有者との照合を行なう際に、その本人の暗証番号PIN(Personal Identification Number)を入力するのに使用されるもので、この暗証番号PINは、カード所有者により任意に設定される所定文字数のコードである。また、このICカード11の本体上面には、さらに接続端子20を設け、銀行等の金融機関あるいは商店の店頭等に設置される上記ターミナル12側との接続を図れるようにする。

次に、第3図により上記ICカード11の回路構成について説明する。

同図において21はバスラインで、このバスライン21には、システム制御部22、システムROM23、キーボード16の制御を行なう入力制御部24、表示部17の制御を行なう表示制御部25および演算制御部26が接続される。また、このバスライン21には、PINメモリ27、PINラッチ部28、フラグレジスタ29およびPANメモリ30が接続される。上記PINメモリ27には、本カード11の発行時において、カード所有者本人が設定した暗証番号(PIN)が予め記憶され、また、PINラッチ部28は、上記キーボード16にてPINキー19を使用してキー入力される所定文字数の情報をラッチするもので、このPINラッチ部28と上記PINメモリ27とをそれぞれ暗証情報比較部31に接続し、この比較部31からの比較照合出力を上記システム制御部22に供給する。この場合、システム制御部22は、上記比較部31による比較照合出力

が一致判定出力であるか否かで、上記フラグレジスタ29に対してフラグ“1”または“0”を立てさせる。一方、上記PANメモリ30には、予めカード発行者により設定される口座番号PAN(Primary Account Number)およびこの口座番号PANが特定のアルゴリズムにて暗号化された暗号化口座番号PAN'が記憶されるもので、この暗号化口座番号PAN'は、後述するPUK(Public Key Code)により解読されるものである。ここで、上記PINメモリ27およびPANメモリ30はそれぞれEPROMにて構成され、一方、PINラッチ部28およびフラグレジスタ29は、それぞれRAMにて構成される。そしてさらに、上記バスライン21には、インターフェイス部32を介して接続端子20を接続する。このようなシステム制御部22乃至インターフェイス部32にて構成されるカード回路は、単独ではソーラ電池18による電源電圧V_{DD}により、また、上記ターミナル12との接続時においては、ターミナル

12側から上記接続端子20を介して供給される電源電圧V_{DD}により駆動される。この場合、上記キーボード16によるPINキー19を使用した所定文字数情報のキー入力動作は、上記ターミナル12との接続時における電源供給時には、絶対に行なわれないように構成する。

次に、第4図により上記ICカードターミナル12の回路構成について説明する。

同図において41はバスラインで、このバスライン41には、システムROM42、システム制御部43、キーボード13を制御する入力制御部44、表示部14を制御する表示制御部45および上記第3図におけるフラグレジスタ29にフラグ“1”が立ったか否かを判断するフラグ判断部46が接続される。この判断部46によるフラグ判断信号は、上記システム制御部43に供給される。また、このバスライン41には、本ターミナル12に接続されるICカード11からのPANデータをラッチするPANラッチ部47および暗号化口座番号PAN'を解読するための解読部

48が接続される。この解読部48には、上述した暗号解読用のキーコードを記憶するPUKメモリ49を接続し、このメモリ内のキーコードによって解読した口座番号を(PAN')として解読PANラッチ部50にラッチさせる。そして、この解読PANラッチ部50および上記PANラッチ部47を、それぞれ口座番号比較部51に接続し、この比較部51からの比較照合信号を上記システム制御部43に供給する。そしてさらに、上記バスライン41には、インターフェイス部52を介して接続端子53が接続される。この接続端子53は、上記第1図におけるカード挿入口15内に設けられ、電源制御部54からの電源電圧V_{DD}の供給ラインが接続される。そして、上記のようにシステムROM42乃至インターフェイス部52により構成されたターミナル回路は、上記電源制御部54からの電源電圧V_{PP}により駆動される。

次に、上記実施例方式にてICカード11の正當性およびカード所有者が本人か否かを順次照合

確認する場合の動作を、第5図および第6図に示すフローチャートを参照して説明する。

第5図はICカードターミナル12内のフローチャートを、第6図はICカード11内のフローチャートを示すもので、まず始めに、ICカード11は、ソーラ電池18による単独の動作状態において、ステップB1に示すように、ターミナル12側からの電源電圧V_{DD}の供給が有るか否かを常に検出し判断する。このステップB2においてN(No)、つまりターミナル12とは接続状態にないと判断されている場合には、ステップB2に進み、キーボード16によるキー入力データは通常の電卓機能により処理される。

ここで、ステップA1において、ICカードターミナル12のカード挿入口15に対してICカード11の一端を挿入し、カード側の接続端子20とターミナル側の接続端子53との電気的接続を図ると、ステップA2に進み、ターミナル側の電源制御部54からカード側に対する電圧V_{DD}の電源供給が開始される。すると、上記カ

ード側のステップB1においてはY(Yes)、つまり電源電圧V_{DD}が供給されターミナル12との完全接続状態に至ったと判断されると、ステップB3に進み、PANメモリ30より取出した口座番号PANおよび暗号化口座番号PAN'を、インターフェイス部32を介してターミナル側に送信する。すると、ターミナル側では、ステップA3において、上記カード側より送られて来るPANおよびPAN'を受信し、PANをPANラッチ部47に、PAN'を解読部48に送込む。この解読部48では、ステップA4において、PUKメモリ49に記憶される暗号解読用のキーコードに基づき上記暗号化口座番号PAN'を解読し、解読PANラッチ部50に(PAN')としてラッチさせるもので、この後ステップA5に進み、口座番号比較部51は、上記PANラッチ部47にラッチされる口座番号PANと解読PANラッチ部50にラッチされる解読口座番号(PAN')とを比較照合する。このステップA5においてY(Yes)、つまりカード側より

送られて来るPANと本ターミナルにて解読した(PAN')とが一致し、現在接続中のICカードは正当なものであると判定されると、ステップA6に進み、システム制御部43は表示部14に対してカードOKメッセージ(OK!)を表示させる。これにより、まず、上記ICカード11は、例えば銀行等により正規に発行された正当なICカードであることが確認される。

この後、ステップA7に進んで、ICカードターミナル12よりICカード11を抜き、各接続端子20-54間を非接続状態とすると、ターミナル12の電源制御部54によるICカード11に対する電源電圧V_{DD}の供給は停止され、ステップB4においてY(Yes)と判断される。そして、次に、ステップB6に進み、ICカード11のキーボード16よりPINキー19を使用して暗証番号PINをキー入力する。すると、このキー入力によるPINはPINラッチ部28に送込まれてラッチされ、そして、このPINラッチ部28にてラッチしたキー入力によるPINと

PINメモリ27により予め記憶される本カード11の真の所有者の暗証番号(PIN)とが、ステップB7において、暗証情報比較部31にて照合比較される。ここで、Y(Yes)、つまり、上記PINと(PIN)とが一致し、上記ステップB6におけるPINのキー入力者は、本カード11の真の所有者であると判定されると、ステップB8に進み、システム制御部22は表示部17に対して本人OKメッセージ(OK!)を表示させる。これにより、現在本カード11を手にしている本人が、真のカード所有者であることが確認されるようになり、上記ステップA6におけるカード正当性の確認とあいまって、カード所有者の正当性は確実なものとなる。

一方、上記ステップA5においてN(No)、つまり接続中のカードより送られたPANと本ターミナルにて解読した(PAN')とが一致せず、現在接続されているカード11は正規に発行されたものではないと判定されると、ステップA8に進み、システム制御部43は表示部14に対して

カード不可メッセージ (BAD) を表示させる。これにより、上記 IC カード 11 は、例えば偽造された假り物の可能性が高いことが確認される。よって、本カード 11 の所有者も、このステップ A8 の時点において、正当な所有者ではないことが判明する。

さらに、上記ステップ A6 において OK メッセージが表示されたとしても、上記ステップ B7 において N (No)、つまり IC カード 11 においてキー入力した PIN と予め記憶される真の PIN とが一致しないと判定されると、ステップ B9 に進み、システム制御部 22 は表示部 17 に対して本人不可メッセージ (BAD) を表示させる。これにより、本 IC カード 11 が上記ターミナル 12 に正規に対応するものであっても、その所有者自体が真の所有者ではないことが確認されるようになる。この場合、本カード 11 は、例えば盗難に合った可能性が高いことが判明する。

次に、上記実施例方式にて IC カード 11 の正当性およびカード所有者が本人か否かを、上記動

作とは逆に順次照合確認する場合の動作を、第 7 図および第 8 図に示すフローチャートを参照して説明する。

まず、ステップ D1 において、IC カード 11 のキーボード 16 より PIN キー 19 を使用して暗証番号 PIN をキー入力する。すると、このキー入力による PIN は PIN ラッチ部 28 に送込まれてラッチされ、そして、この PIN ラッチ部 28 にてラッチしたキー入力による PIN と PIN メモリ 27 により予め記憶される本カード 11 の真の所有者の暗証番号 (PIN) とが、ステップ D2 において、暗証情報比較部 31 にて照合比較される。ここで、Y (Yes)、つまり、上記 PIN と (PIN) とが一致し、上記ステップ D1 における PIN のキー入力者は、本カード 11 の真の所有者であると判定されると、ステップ D3 に進み、システム制御部 22 はフラグレジスタ 29 に対してフラグ "1" を立てさせる。この後、ステップ D4 に進み、カード 11 側ではターミナル 12 側からの電源電圧 V_{DD} の供給が有

るか否かを常に検出し判断する。ここで、ステップ C1 において、IC カードターミナル 12 のカード挿入口 15 に対して IC カード 11 の一端を挿入し、カード側の接続端子 20 とターミナル側の接続端子 53 との電気的接続を図ると、ステップ D2 に進み、ターミナル側の電源制御部 54 からカード側に対する電圧 V_{DD} の電源供給が開始される。すると、上記カード側のステップ D4 においては Y (Yes)、つまり電源電圧 V_{DD} が供給されターミナル 12 との完全接続状態に至ったと判断されると、ステップ D5 に進み、PAN メモリ 30 より取出した口座番号 PAN および暗号化口座番号 PAN' を、インターフェイス部 32 を介してターミナル側に送信する。すると、ターミナル側では、ステップ C3 において、上記カード側より送られて来る PAN および PAN' を受信し、PAN を PAN ラッチ部 47 に、PAN' を解読部 48 に送込む。この解読部 48 では、ステップ C4 において、PUK メモリ 49 に記憶される暗号解読用のキーコードに基づき上記暗号化

口座番号 PAN' を解読し、解読 PAN ラッチ部 50 に (PAN') としてラッチさせるもので、この後ステップ C5 に進み、口座番号比較部 51 は、上記 PAN ラッチ部 47 にラッチされる口座番号 PAN と解読 PAN ラッチ部 50 にラッチされる解読口座番号 (PAN') とを比較照合する。このステップ C5 において Y (Yes)、つまりカード側より送られて来る PAN と本ターミナルにて解読した (PAN') とが一致し、現在接続中の IC カードは正当なものであると判定されると、ステップ C6 に進み、システム制御部 43 は上記 IC カード 11 に対してフラグ要求信号を出力する。すると、カード側では、ステップ D6 において上記ターミナル 12 側からのフラグ要求信号を受信し、ステップ D7 に進んで、上記ステップ D3 にてフラグレジスタ 29 に立てたフラグ "1" をターミナル側に送信する。すると、ターミナル 12 側では、ステップ C7 において上記カード 11 側からのフラグ信号を受信し、このフラグ信号には "1" が立っているか否かをステップ

C8にて判断する。このステップC8においてY (Yes)、つまり、上記ステップC5において、現在接続中のICカード11が正当なものであると判定されただけでなく、上記ステップD2において、既に上記ステップD1におけるPINのキー入力者は、本カード11の真の所有者であると判定されていると判断されると、ステップC9に進み、システム制御部43は表示部14に対してカードOKメッセージ(OKI)を表示させる。これにより、ICカード11自体が正規に発行された本物であることおよびそのカードの持主が所有者本人であることが何れも判明することとなり、カード所有者の正当性は確実なものとなる。

一方、上記ステップD2においてN(No)、つまりICカード11においてキー入力したPINと予め記憶される真のPINとが一致しないと判定されると、ステップD8に進み、システム制御部22はフラグレジスタ29に対してフラグ“0”を立てさせる。この場合、上記ステップC5に進んだ時点においてY(Yes)、つまりカ

は偽造された假物の可能性が高いことが確認される。よって、本カード11の所有者も、このステップC10の時点において、正当な所有者ではないことが判明する。

したがってこのように構成されるICカードにおける本人照合方式によれば、ICカード11の所有者は真の所有者であるか否かだけでなく、そのカード自体が銀行等により正規に発行されたものであるか否かをも確認することができるので、カード利用者の正当性を確実に証明することが可能である。また、上記ICカード11における暗証番号PINの比較照合動作は、カードターミナル12との接続時においては実行されないように構成されているので、万一、カードターミナル側に何等かの細工が施してあったとしても、カード利用者の暗証情報が盗まれる恐れは全くない。

〔発明の効果〕

以上のようにこの発明によれば、外部装置との接続によりカード自体の正当性が確認できるICカード内に、所定文字数の暗証情報を予め記憶す

ード側より送られて来るPANと本ターミナルにて解読した(PAN')とが一致し、現在接続中のICカードは正当なものであると判定されても、ステップC8においてN(No)と判定され、ステップC10に進む。このステップC10において、システム制御部43は表示部14に対してカード不可メッセージ(BAD)を表示させるもので、これにより、本ICカード11が上記ターミナル12に正規に対応するものであっても、その所有者自体が真の所有者ではないことが確認されるようになる。この場合、本カード11は、例えば盗難に合った可能性が高いことが判明する。

さらに、上記ステップC5においてN(No)、つまり接続中のカードより送られたPANと本ターミナルにて解読した(PAN')とが一致せず、現在接続されているカード11は正規に発行されたものではないと判定されると、上記ステップC10に進み、システム制御部43は表示部14に対してカード不可メッセージ(BAD)を表示させる。これにより、上記ICカード11は、例え

る暗証情報メモリを設けると共に、上記外部装置との非接続状態において上記所定文字数情報の入力可能な手段を備えさせ、そして、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをこのICカード内にて独自に比較照合し、その照合結果を出力するように構成したので、カード所有者の暗証情報が不正に盗まれてしまうことなく、カード所有者の正当性を確実に確認することが可能となるICカードにおける本人照合方式を提供できる。

4. 図面の簡単な説明

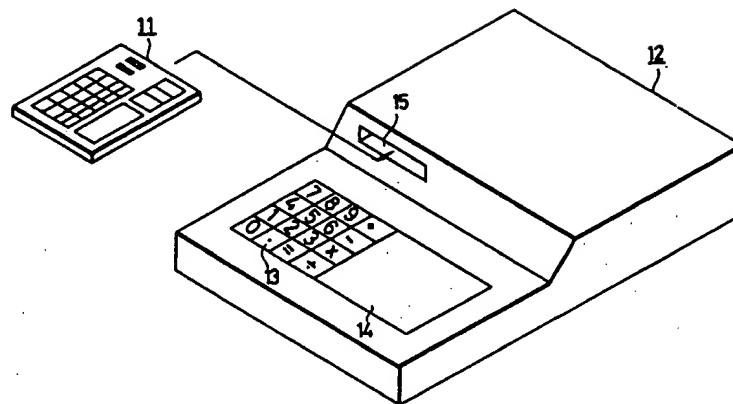
第1図はこの発明の一実施例に係わるICカードにおける本人照合方式を実現した場合のICカードターミナルを示す外観構成図、第2図は上記第1図におけるICカードを拔出して示す外観構成図、第3図は上記ICカードにおける本人照合方式を実現した場合のICカードを示す回路構成図、第4図は上記ICカードにおける本人照合方式を実現した場合のICカードターミナルを示す回路構成図、第5図および第6図はそれぞれ上記

ICカードにおける本人照合方式によりICカードの正当性およびカード所有者が本人か否かを順次照合確認する場合の動作を示すICカードターミナル（外部装置）側およびICカード側のフローチャート、第7図および第8図はそれぞれ上記ICカードにおける本人照合方式によりICカードの正当性およびカード所有者が本人か否かを上記第5図および第6図に示した場合とは逆に順次照合確認する場合の動作を示すICカードターミナル（外部装置）側およびICカード側のフローチャートである。

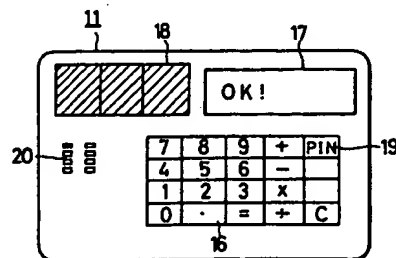
47…PANラッチ部、48…解読部、49…PUKメモリ、50…解読PANラッチ部、51…口座番号比較部、53…ターミナル接続端子、54…電源制御部。

出願人 カシオ計算機株式会社

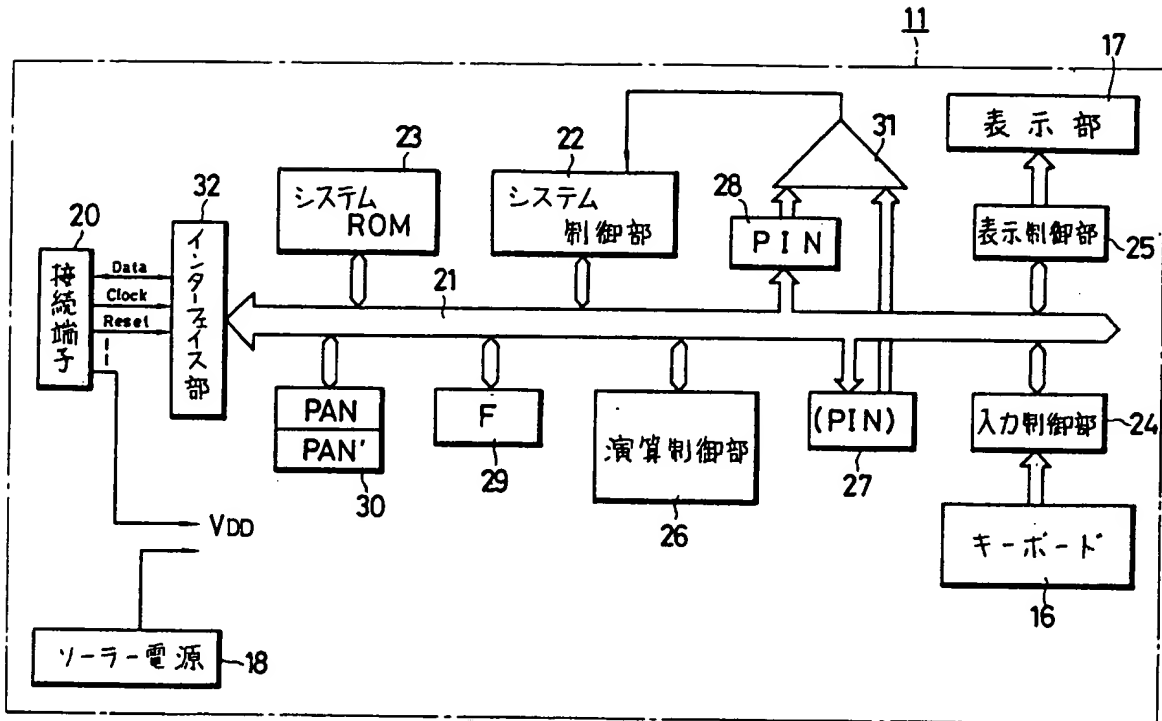
11…ICカード、12…ICカードターミナル（外部装置）、14…ターミナル表示部、15…カード挿入口、16…カードキーボード、17…カード表示部、18…ソーラ電池、19…PINキー、20…カード接続端子、22…カードシステム制御部、27…PINメモリ、28…PINラッチ部、29…フラグレジスタ、30…PANメモリ、31…暗証情報比較部、43…ターミナルシステム制御部、46…フラグ判断部、



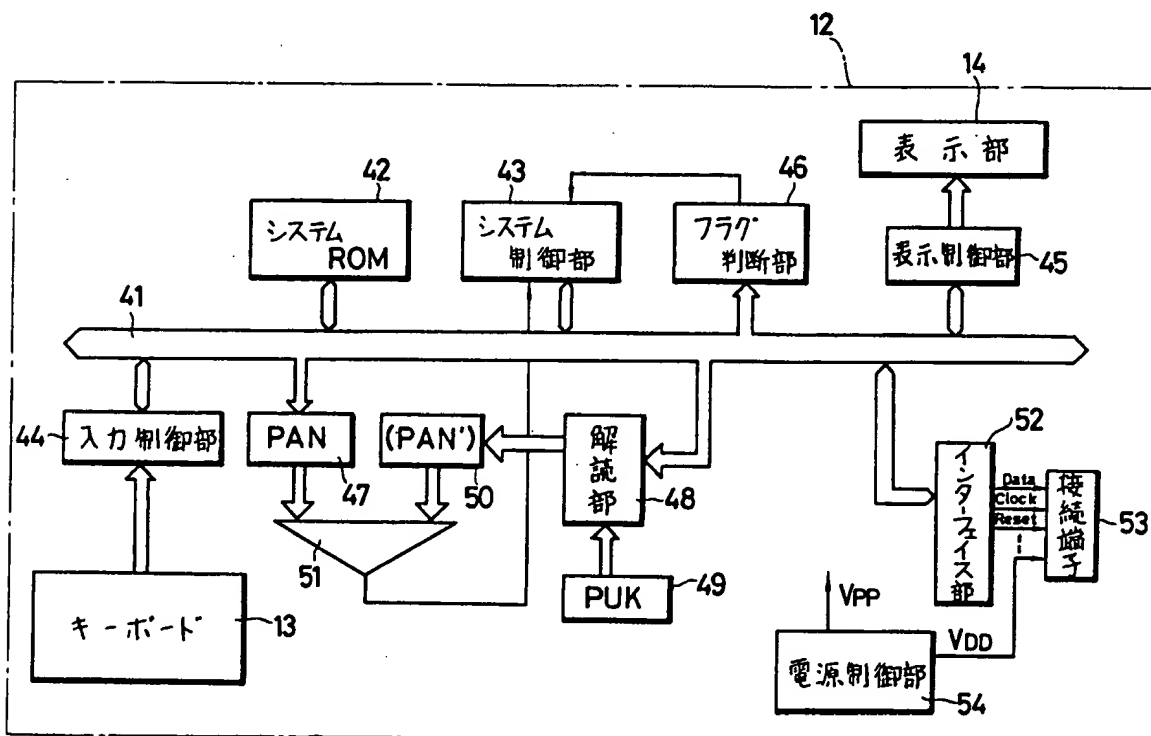
第1図



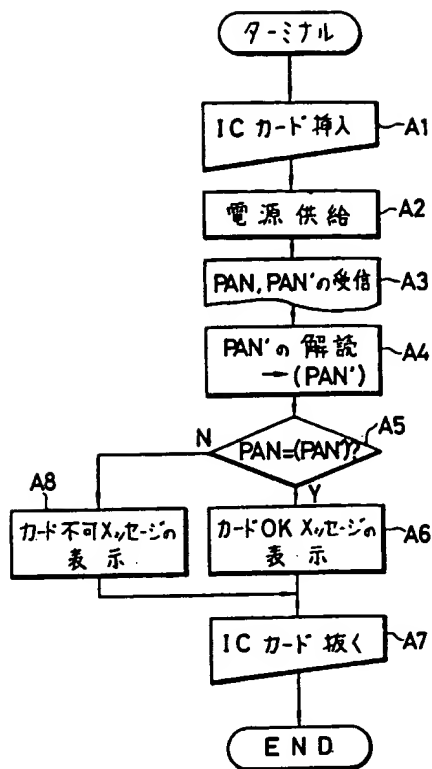
第2図



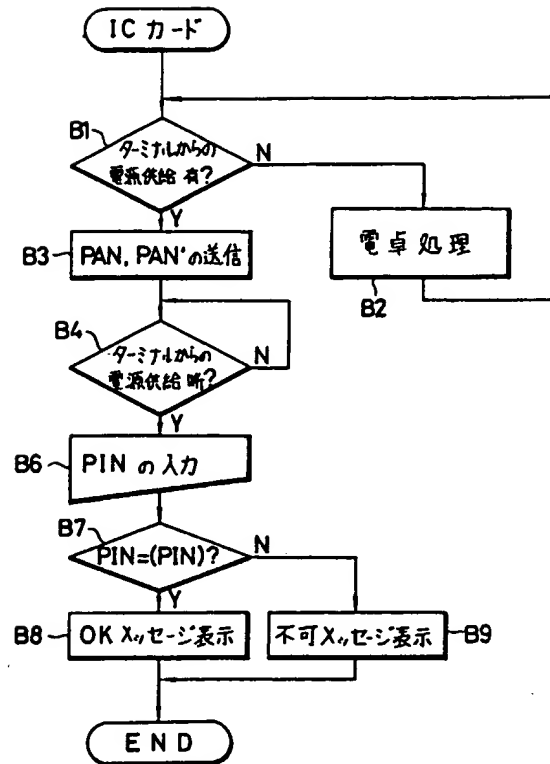
第 3 図



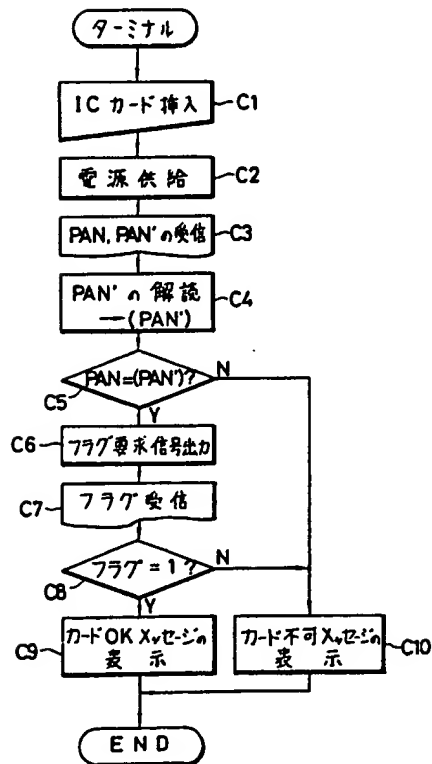
第 4 図



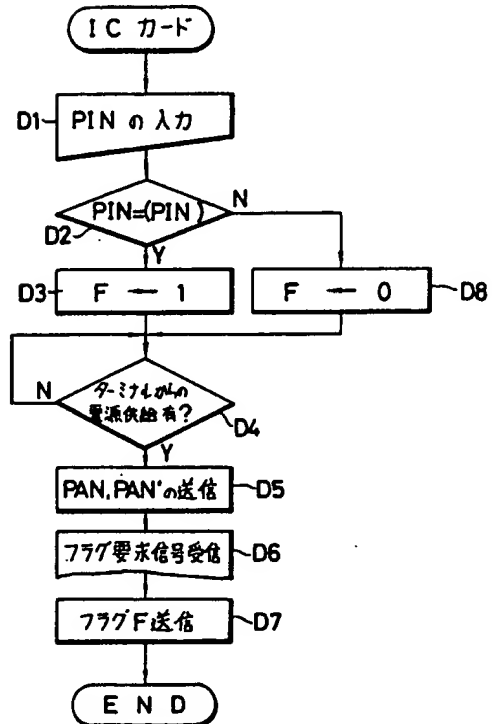
第 5 図



第 6 図



第 7 図



第 8 図